IN THE CLAIMS

Cancel claims 1, 8-10, 13, 18, 25, 26, 35, 38, 45-47, 50, 53, 60, 61 and 70; and amend the remaining claims as noted in the following listing of the claims.

1. (Canceled)

2. (Currently Amended) An enciphering apparatus ~~according to claim 1,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information;

second providing means for providing second information which is changed during a session;

producing means for producing a cryptographic key based on the first information and the second information; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the session in accordance with a change in said second information; and

wherein said producing means produces a homomorphic cryptographic key.

3. (Currently Amended) An enciphering apparatus ~~according to claim 1,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information;

second providing means for providing second information which is changed during a session;

producing means for producing a cryptographic key based on the first information and the second information; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the session in accordance with a change in said second information; and

wherein said producing means produces said cryptographic key with which a correct decipherment result is obtained even if the first information and the second information which are used to generate said cryptographic key are used individually to successively decipher the enciphered data.

4. (Currently Amended) An enciphering apparatus ~~according to claim 1,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information;

second providing means for providing second information which is changed during a session;

producing means for producing a cryptographic key based on the first information and the second information; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the session in accordance with a change in said second information; and

wherein said producing means adds the second information to a value whose initial value is the first information to produce the cryptographic key.

5. (Previously Presented) An enciphering apparatus according to claim 4, wherein the first information has a number of bits larger than that of the second information, and said producing means adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

6. (Original) An enciphering apparatus according to claim 5, wherein said producing means further updates the predetermined bits of the result of the addition with a result of the further addition of the extracted bit.

7. (Original) An enciphering apparatus according to claim 6, wherein said producing means selects predetermined bits from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (Currently Amended) A deciphering apparatus ~~according to claim 10,~~ for deciphering data using a cryptographic key, comprising:

receiving means for receiving enciphered data;

first providing means for providing first information;

second providing means for providing second information which is changed during a session;

producing means for producing a cryptographic key based upon the first information and the second information; and

deciphering means for deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the session in accordance with a change in said second information and

wherein said producing means includes first producing means for producing a first cryptographic key based upon one of the first information and the second information, and

second producing means for producing a second cryptographic key based upon the other of the first information and the second information, and said deciphering means includes first deciphering means for deciphering the enciphered data based upon the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further based upon the second cryptographic key.

12. (Original) A deciphering apparatus according to claim 11, wherein said second deciphering means is formed from application software for processing the deciphered data.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Currently Amended) An information processing apparatus, comprising:

receiving means for receiving enciphered data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second cryptographic key based upon ~~a~~ first information and ~~a~~ second information which is changed during ~~the~~a predetermined session;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second

cryptographic key produced by said producing means, wherein said second cryptographic key is changed while said data is being deciphered.

17. (Currently Amended) An information processing method, comprising the steps of:

receiving enciphered data transmitted thereto through a bus;

producing, from the received data, a first cryptographic key, and a second cryptographic key based upon ~~a~~ first information and ~~a~~ second information which is changed during ~~the predetermined~~a session;

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second cryptographic key, wherein said second cryptographic key is changed while said data is being deciphered.

18. (Canceled)

19. (Currently Amended) The enciphering apparatus ~~according to claim 18,~~ for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and second information provided by said second information provider and changed at a predetermined timing during a session and

wherein said cryptographic key producer produces a homomorphic cryptographic key.

20. (Currently Amended) The enciphering apparatus ~~according to claim 18,~~ for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and second information provided by said second information provider and changed at a predetermined timing during a session and

wherein said cryptographic key producer produces said cryptographic key with which a correct decipherment result is obtained even if ~~a~~the first information and ~~a~~the second information on which ~~compose~~ the cryptographic key is based are used individually to successively decipher the enciphered data.

21. (Currently Amended) The enciphering apparatus ~~according to claim 18,~~ for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and second

information provided by said second information provider and changed at a predetermined timing during a session and

wherein said cryptographic key producer adds the second information to a value whose initial value is the first information to produce the cryptographic key.

22. (Previously Presented) The enciphering apparatus according to claim 21, wherein the first information has a number of bits larger than that of the second information, and said cryptographic key producer adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

23. (Previously Presented) The enciphering apparatus according to claim 22, wherein said cryptographic key producer further updates the result of the addition with the further addition of the extracted bit.

24. (Previously Presented) The enciphering apparatus according to claim 23, wherein said cryptographic key producer selects predetermined bits from a result of the further addition of the extracted bits at a predetermined timing to produce the cryptographic key.

25. (Canceled)

26. (Canceled)

27. (Previously Presented) The deciphering apparatus ~~according to claim 26,~~ for deciphering data using a cryptographic key, comprising:

a receiver;

a decipherer coupled with said receiver;

a first information provider coupled with said decipherer;

a second information provider coupled with said decipherer; and

a cryptographic key producer coupled with said decipherer, whereby said decipherer deciphers data received by said receiver using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and second information provided by said second information provider and changed at a predetermined timing during a session,

wherein said cryptographic key producer includes a first cryptographic key producer coupled with said first and second information providers for producing a first cryptographic key using one of the first information and the second information, and a second cryptographic key producer coupled with said first and second information providers and said first cryptographic key producer for producing a second cryptographic key using the other of the first information and the second information, and said decipherer includes a first deciphering section and a second deciphering section, said first deciphering section deciphering the enciphered data using the first cryptographic key, and said second deciphering section deciphering the data deciphered by said first deciphering section using the second cryptographic key.

28. (Previously Presented) The deciphering apparatus according to claim 27, wherein said second deciphering section is formed from application software for processing the deciphered data.

29. (Currently Amended) An enciphering method ~~according to claim 9,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information;

providing second information which is changed during a session;

producing a cryptographic key based upon the first information and the second information; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during a session in accordance with a change in said second information and

wherein a homomorphic cryptographic key is produced.

30. (Currently Amended) An enciphering method ~~according to claim 9,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information;

providing second information which is changed during a session;

producing a cryptographic key based upon the first information and the second information; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during a session in accordance with a change in said second information and

wherein said cryptographic key is produced with which a correct decipherment result is obtained even if the first information and the second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

31. (Currently Amended) An enciphering method ~~according to claim 9,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information;

providing second information which is changed during a session;

producing a cryptographic key based upon the first information and the second information; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during a session in accordance with a change in said second information and

wherein the second information is added to a value whose initial value is the first information to produce the cryptographic key.

32. (Previously Presented) An enciphering method according to claim 31, wherein the first information has a number of bits larger than that of the second information, and the second information is added to bits at predetermined positions of the first information, a bit at a predetermined position of a result of the addition is extracted and the extracted bit is further added to produce the cryptographic key.

33. (Previously Presented) An enciphering method according to claim 32, wherein the predetermined bits of the result of the addition are updated with a result of the further addition of the extracted bit.

34. (Previously Presented) An enciphering method according to claim 33, wherein predetermined bits are selected from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

35. (Canceled)

36. (Currently Amended) A deciphering method ~~according to claim 13,~~ for deciphering data using a cryptographic key, comprising the steps of:

receiving enciphered data;

providing first information;

providing second information which is changed during a session;

producing a cryptographic key based upon the first information and the second information; and

deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during a session in accordance with a change in said second information and

wherein a first cryptographic key is produced using one of the first information and the second information, and a second cryptographic key is produced using the other of the first information and the second information, and the enciphered data is first deciphered using the first cryptographic key, the data deciphered using the first cryptographic key is further deciphered using the second cryptographic key.

37. (Previously Presented) A deciphering apparatus according to claim 36, wherein deciphering using said second cryptographic key is performed by application software for processing the deciphered data.

38. (Canceled)

39. (Currently Amended) An enciphering apparatus ~~according to claim 38,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing second information which is changed at a predetermined timing;

producing means for producing the cryptographic key based on the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information and

wherein said producing means produces a homomorphic cryptographic key.

40. (Currently Amended) An enciphering apparatus ~~according to claim 38,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing second information which is changed at a predetermined timing;

producing means for producing the cryptographic key based on the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information and

wherein said producing means produces said cryptographic key with which a correct decipherment result is obtained even if the first information and the second information which are used to generate said cryptographic key are used individually to successively decipher the enciphered data.

41. (Currently Amended) An enciphering apparatus ~~according to claim 38,~~ for enciphering data using a cryptographic key, comprising:

first providing means for providing first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing second information which is changed at a predetermined timing;

producing means for producing the cryptographic key based on the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering means for enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information and

wherein said producing means adds the second information to a value whose initial value is the first information to produce the cryptographic key.

42. (Previously Presented) An enciphering apparatus according to claim 41, wherein the first information has a number of bits larger than that of the second information, and said producing means adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

43. (Previously Presented) An enciphering apparatus according to claim 42, wherein said producing means further updates the predetermined bits of the result of the addition with a result of the further addition of the extracted bit.

44. (Previously Presented) An enciphering apparatus according to claim 43, wherein said producing means selects predetermined bits from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

45. (Canceled)

46. (Canceled)

47. (Canceled)

48. (Currently Amended) A deciphering apparatus ~~according to claim 47,~~ for deciphering data using a cryptographic key, comprising:

receiving means for receiving enciphered data;

first providing means for providing first information which is held in common with another device in an authentication process by communication between the two devices;

second providing means for providing second information which is changed at a predetermined timing;

producing means for producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

deciphering means for deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information and

wherein said producing means includes first producing means for producing a first cryptographic key based upon one of the first information and the second information, and second producing means for producing a second cryptographic key based upon the other of the first information and the second information, and said deciphering means includes first deciphering means for deciphering the enciphered data based upon the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further based upon the second cryptographic key.

49. (Previously Presented) A deciphering apparatus according to claim 48, wherein said second deciphering means is formed from application software for processing the deciphered data.

50. (Canceled)

51. (Currently Amended) An information processing apparatus, comprising:

receiving means for receiving enciphered data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second cryptographic key based upon ~~a~~ first information which is held in common with another device in an authentication process by communication between the two devices and ~~a~~ second information which is changed at a predetermined timing~~while the data is being deciphered~~;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second cryptographic key produced by said producing means, wherein said second cryptographic key is changed in accordance with said second information at a predetermined timing~~while said data is being deciphered~~.

52. (Currently Amended) An information processing method, comprising the steps of:

receiving enciphered data transmitted thereto through a bus;

producing, from the received data, a first cryptographic key, and a second cryptographic key based upon ~~a~~ first information held in common with another device in an

authentication process by communication between the two devices and ~~a~~ second information which is changed at a predetermined timing~~while the data is being deciphered~~;

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second cryptographic key, wherein said second cryptographic key is changed in accordance with the second information at a predetermined timing~~while said data is being deciphered~~.

53. (Canceled)

54. (Currently Amended) ~~The enciphering apparatus according to claim 53,~~ An enciphering apparatus for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and held in common with another device in an authentication process by communication between the two devices, and second information provided by said second information provider and changed at a predetermined timing

wherein said cryptographic key producer produces a homomorphic cryptographic key.

55. (Currently Amended) ~~The enciphering apparatus according to claim 53,~~ An enciphering apparatus for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and held in common with another device in an authentication process by communication between the two devices, and second information provided by said second information provider and changed at a predetermined timing

wherein said cryptographic key producer produces said cryptographic key with which a correct decipherment result is obtained even if a first information and a second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

56. (Currently Amended) ~~The enciphering apparatus according to claim 53,~~ An enciphering apparatus for enciphering data using a cryptographic key, comprising:

an encipherer;

a first information provider coupled with said encipherer;

a second information provider coupled with said encipherer; and

a cryptographic key producer coupled with said encipherer, whereby said encipherer enciphers data using a cryptographic key produced by said cryptographic key producer based upon first information provided by said first information provider and held in common with another device in an authentication process by communication between the two devices, and second information provided by said second information provider and changed at a predetermined timing.

wherein said cryptographic key producer adds the second information to a value whose initial value is the first information to produce the cryptographic key.

57. (Previously Presented) The enciphering apparatus according to claim 56, wherein the first information has a number of bits larger than that of the second information, and said cryptographic key producer adds the second information to bits at predetermined positions of the first information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

58. (Previously Presented) The enciphering apparatus according to claim 57, wherein said cryptographic key producer further updates the result of the addition with the further addition of the extracted bit.

59. (Previously Presented) The enciphering apparatus according to claim 58, wherein said cryptographic key producer selects predetermined bits from a result of the further addition of the extracted bits at a predetermined timing to produce the cryptographic key.

60. (Canceled)

61. (Canceled)

62. (Currently Amended) ~~The deciphering apparatus according to claim 61,~~ A deciphering apparatus for deciphering data using a cryptographic key, comprising:

a receiver;

a decipherer coupled with said receiver;

a first information provider coupled with said decipherer;

a second information provider coupled with said decipherer; and

a cryptographic key producer coupled with said decipherer, whereby said decipherer deciphers data received by said receiver using a cryptographic key produced by said

cryptographic key producer based upon first information provided by said first information provider and held in common with another device in an authentication device by communication between the two devices and second information provided by said second information provider and changed at a predetermined timing.

wherein said cryptographic key producer includes a first cryptographic key producer coupled with said first and second information providers for producing a first cryptographic key using one of the first information and the second information, and a second cryptographic key producer coupled with said first and second information providers and said first cryptographic key producer for producing a second cryptographic key using the other of the first information and the second information, and said decipherer includes a first deciphering section and a second deciphering section, said first deciphering section deciphering the enciphered data using the first cryptographic key, and said second deciphering section deciphering the data deciphered by said first deciphering section using the second cryptographic key.

63. (Previously Presented) The deciphering apparatus according to claim 62, wherein said second deciphering section is formed from application software for processing the deciphered data.

64. (Currently Amended) An enciphering method~~according to claim 46,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information which is held in common with another device in an authentication process by communication between the two devices;

providing second information which is changed at a predetermined timing;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information, and

wherein a homomorphic cryptographic key is produced.

65. (Currently Amended) An enciphering method ~~according to claim 46,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information which is held in common with another device in an authentication process by communication between the two devices;

providing second information which is changed at a predetermined timing;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information, and

wherein said cryptographic key is produced with which a correct decipherment result is obtained even if the first information and the second information which compose the cryptographic key are used individually to successively decipher the enciphered data.

66. (Currently Amended) An enciphering method ~~according to claim 46,~~ for enciphering data using a cryptographic key, comprising the steps of:

providing first information which is held in common with another device in an authentication process by communication between the two devices;

providing second information which is changed at a predetermined timing;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information, and

wherein the second information is added to a value whose initial value is the first information to produce the cryptographic key.

67. (Previously Presented) An enciphering method according to claim 66, wherein the first information has a number of bits larger than that of the second information, and the second information is added to bits at predetermined positions of the first information, a bit at a predetermined position of a result of the addition is extracted and the extracted bit is further added to produce the cryptographic key.

68. (Previously Presented) An enciphering method according to claim 67, wherein the predetermined bits of the result of the addition are updated with a result of the further addition of the extracted bit.

69. (Previously Presented) An enciphering method according to claim 68, wherein predetermined bits are selected from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

70. (Canceled)

71. (Currently Amended) A deciphering method ~~according to claim 50,~~ for deciphering data using a cryptographic key, comprising the steps of:

receiving enciphered data;

providing first information which is held in common with another device in an authentication process by communication between the two devices;

providing second information which is changed at a predetermined timing;

producing a cryptographic key based upon the first information held in common with the other device and the second information which is used for changing the cryptographic key; and

deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing in accordance with a change in said second information, and

wherein a first cryptographic key is produced using one of the first information and the second information, and a second cryptographic key is produced using the other of the first information and the second information, and the enciphered data is first deciphered using the first cryptographic key, the data deciphered using the first cryptographic key is further deciphered using the second cryptographic key.

72. (Previously Presented) A deciphering apparatus according to claim 71, wherein deciphering using said second cryptographic key is performed by application software for processing the deciphered data.